USB-токен системы «iBank 2».

USB-токен — это аппаратное USB-устройство, состоящее из PC/SC-совместимого USB-кардридера и SIM-карты, в которой реализованы все российские криптоалгоритмы и имеется защищенная область памяти, позволяющая хранить до 64-х секретных ключей ЭЦП.

Рис. 1. USB-токен

В USB-токене реализованы следующие криптографические функции:

- аппаратный криптографически стойкий генератор случайных чисел;
- генерация пары ключей ЭЦП;
- формирование и проверка ЭЦП по ГОСТ Р34.10-2001 (эллиптические кривые);
- генерация ключей шифрования;
- шифрование и расшифрование в соответствии с ГОСТ 28147-89;
- формирование и проверка имитовставки (последовательности данных фиксированной длины, получаемой по определенному правилу из открытых данных и секретного ключа и добавляемой к данным для обеспечения имитозащиты) в соответствии с ГОСТ 28147-89;
- вычисление хеш-функции в соответствии с ГОСТ Р34.11-94.

Формирование ЭЦП клиента в соответствии с ГОСТ Р34.10-2001 непосредственно внутри SIM-карты токена: на вход токен принимает электронный документ, на выходе выдает ЭЦП под данным документом. При этом время формирования токеном ЭЦП приблизительно равно 0,5 сек.

- USB-токены корректно работают на Windows XP Professional / XP Home / 2000 Server / Server 2003 / 2000 Professional / Vista / Windows 7 используется Java 6.

Секретный ключ ЭЦП генерируется самим токеном, хранится в защищенной памяти токена и никогда, никем и ни при каких условиях не может быть считан из токена.

Для использования функций криптографической защиты в USB-токене встроена поддержка криптобиблиотеки СКЗИ «Криптомодуль-С» компании «Терна СБ», сертифицированных ФСБ (сертификат соответствия рег. № СФ/114-1009 от 14 мая 2007 года, действителен до 9 марта 2010 года).

Основные преимущества использования USB-токенов!

1. Безопасность хранения ключа – в связи с тем что ключ ЭЦП генерируется изначально на токене и в течении всей работы с ним никогда его не покидает, хищение ключа фактически невозможно

2. На одном токене возможно сохранение до 64 ключей ЭЦП

3. На токене невозможно сохранить прочую информацию кроме ключа ЭЦП. Тем самым вы обезопасите себя от случайного удаления ключа или перезаписи файла

4. Токен не имеет срока годности и не содержит в себе движущихся (механических устройств) приходящих в негодность со временем.

Установка драйвера для USB-токенов.

Драйвер USB-токена необходим для работы в системе электронного банкинга «iBank 2».

Внимание!

Драйверы USB-токена устанавливаются до подключения устройства. Во время установки драйверов все приложения должны быть закрыты во избежание ошибки разделения файлов. Для установки драйверов пользователю необходимы права администратора системы.

Для установки драйвера USB-токена с сайта банка https://ibank.ccb.ru/jvm.html скачайте и запустите файл iBank2KeySetup.exe. **(https://ibank.ccb.ru/doc/iBank2KeySetup.exe)**
На экране появится окно выбора языка установки (см. рис. 1).

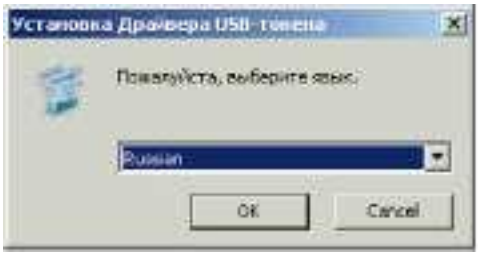


Рис. 1. Выбор языка установки

Выберите требуемый язык и нажмите кнопку ОК для перехода к стартовому окну мастера установки драйвера (см. рис. 2).

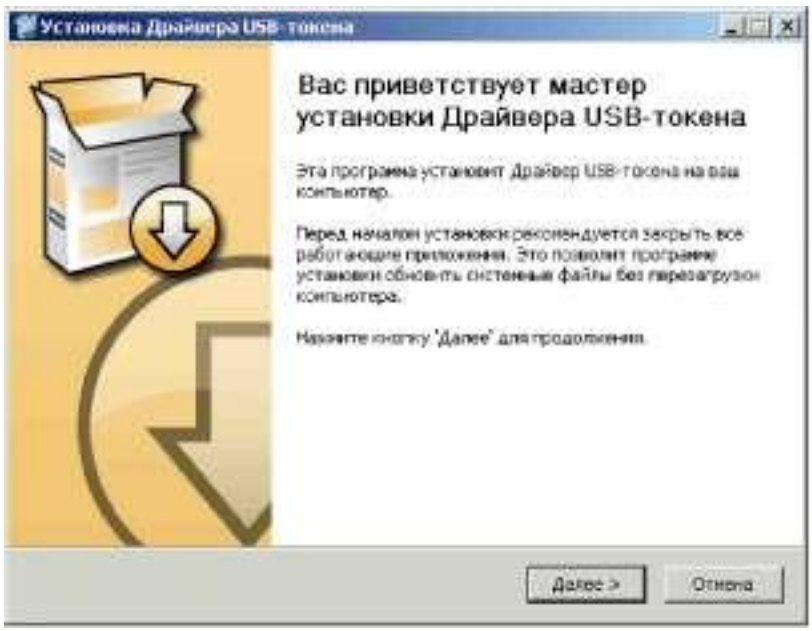


Рис. 2. Стартовое окно мастера установки Драйвера

В этом окне нажмите кнопку Далее для перехода к окну выбора каталога установки (см. рис. 3).

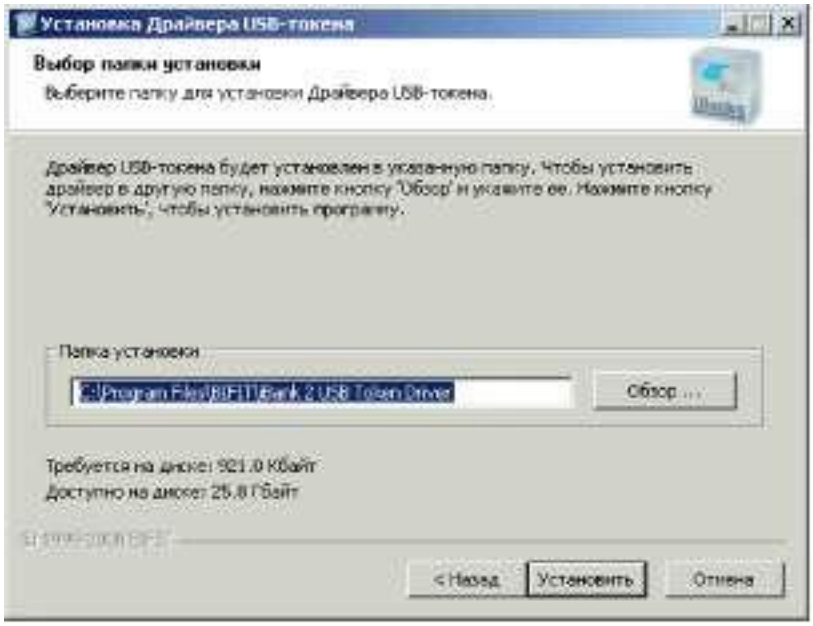


Рис. 3. Выбор каталога установки Драйвера

Введите адрес каталога, в который будет установлен Драйвер USB-токена, в соответствующее поле или выберите его с помощью кнопки **Выбор** (адрес по умолчанию C:\Program Files\BIFIT\iBank 2 USB Token Driver). Нажмите кнопку **Установить.**

После завершения процесса установки в финальном окне диалога установки нажмите кнопку Далее (см. рис. 4).

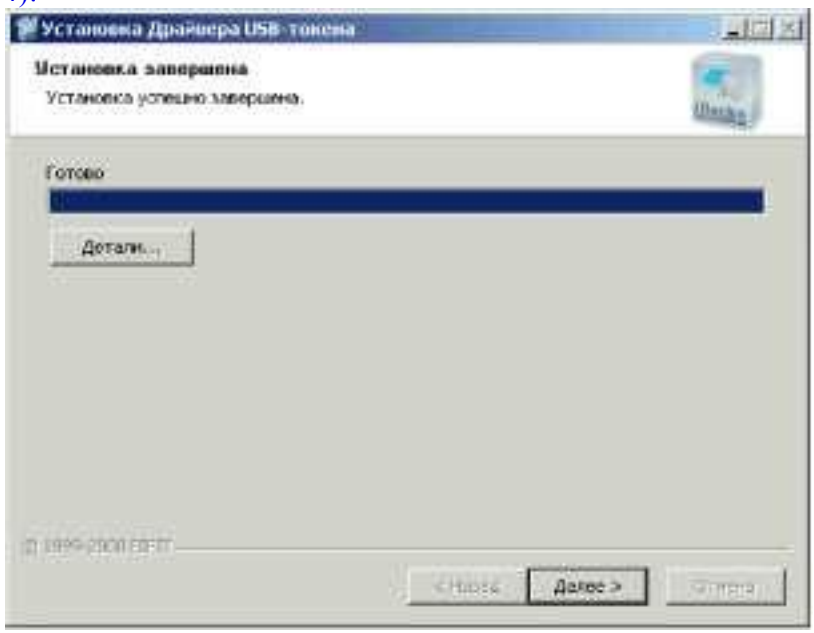
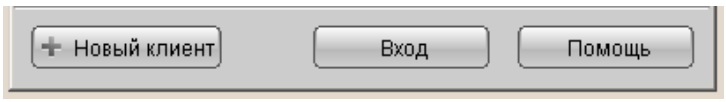


Рис. 4. Финальное окно диалога установки Драйвера

В окне **Завершение работы мастера установки USB-токена** отметьте поле **Показать файл ReadMe** и нажмите кнопку **Готово.**

Установка драйвера USB-токена завершена.

Процесс предварительной регистрации осуществляется в АРМ «Новый клиент – Internet-Банкинг для корпоративных клиентов», который представляет собой Java-апплет. Для его загрузки подключитесь к Интернет, запустите Web-браузер и перейдите на главную страницу системы «iBank 2». На главной странице системы «iBank 2» выберите пункт **«Начать работу / Зарегистрироваться»,** в результате чего сначала загрузится html-страница, содержащая краткое описание, а через 15 — 30 секунд (в зависимости от скорости доступа в Интернет) загрузится АРМ «Новый клиент – Internet-Банкинг для корпоративных клиентов», в нем необходимо выбрать пункт **«+ Новый клиент».**



Подключите USB-токен к USB-порту компьютера. Если все сделано правильно (драйвер установлен) USB-токен будет постоянно гореть синим светом.

Пройдите все этапы регистрации нового клиента. На восьмом шаге в качестве Хранилища ключей выберите из списка **USB-токен.**

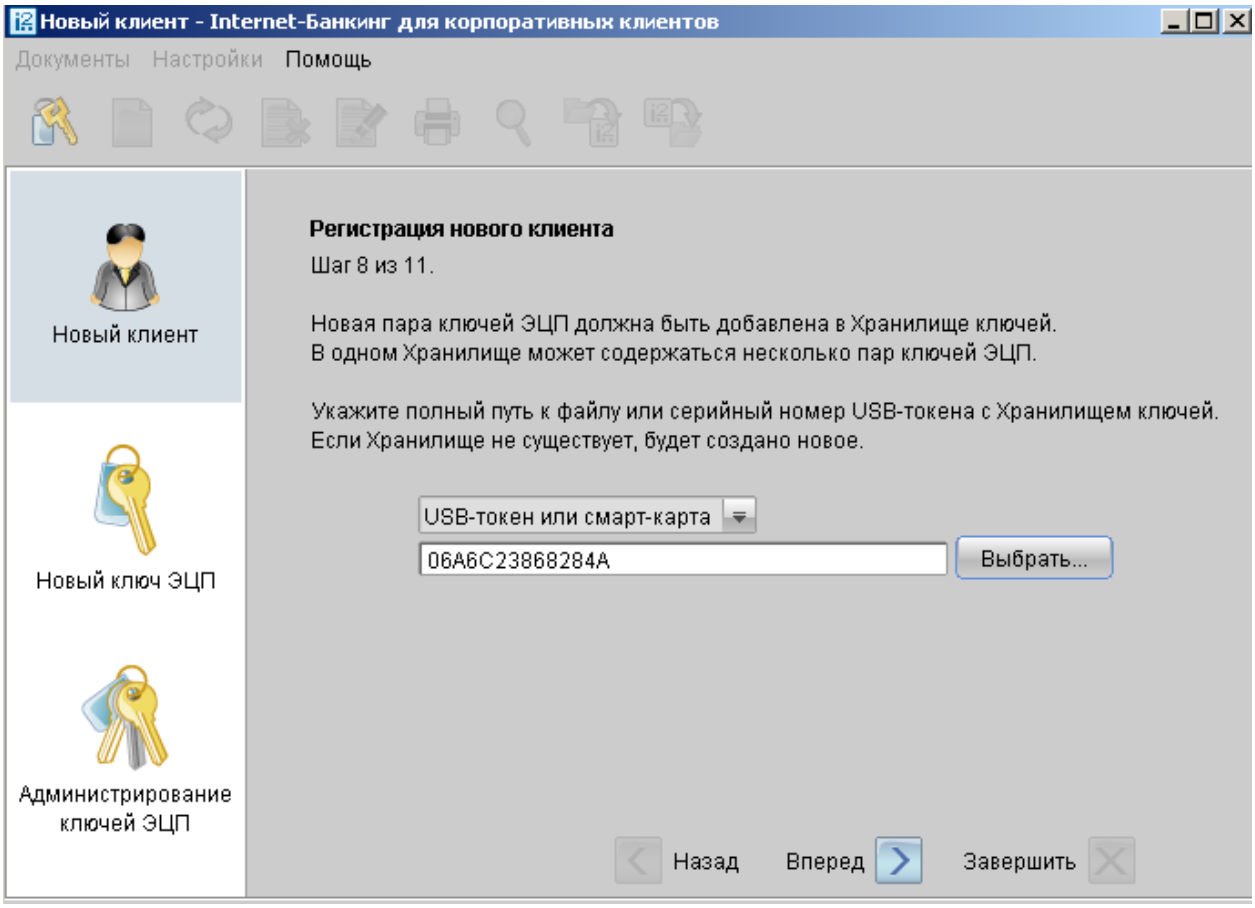


Рис. 6. Предварительная регистрация. Шаг 8 из 11

Примечания:

В одном Хранилище ключей USB-токена может содержаться несколько секретных ключей ЭЦП одного физического лица.

Важно!

Для того чтобы Ваш пароль был безопасным:

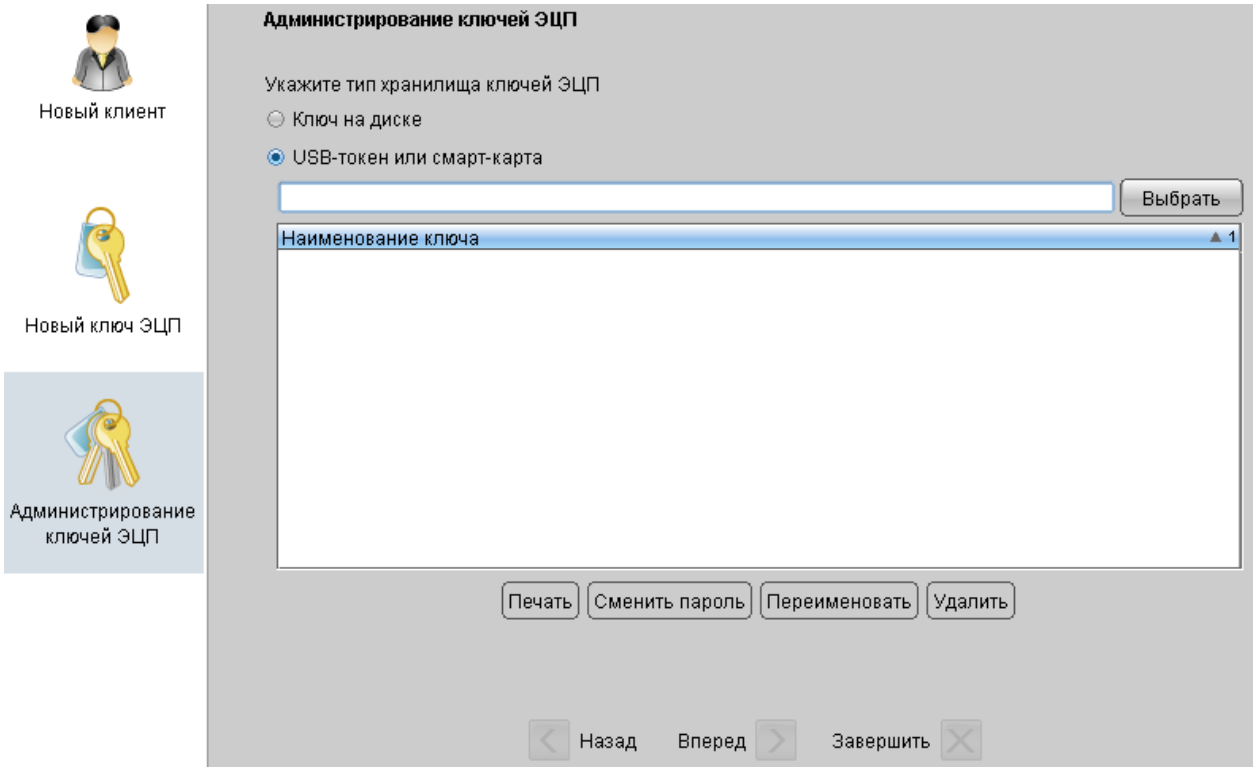
- пароль не должен состоять из одних цифр (так его легче подсмотреть из-за спины);
- пароль не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре;
- пароль должен содержать в себе как заглавные, так и строчные буквы, цифры и знаки препинания;
- пароль не должен быть значимым словом (Ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать или угадать.

Важно!

Неправильно ввести пароль к ключу можно не более 15 раз подряд. После этого ключ блокируется навсегда.

Администрирование USB-токенов клиента осуществляется в АРМ «Новый клиент – Internet-Банкинг для корпоративных клиентов».

Загрузите Java-апплет «Новый клиент – Internet-Банкинг для корпоративных клиентов» и выбираете пункт **«+ Новый клиент».** В левом меню в выберите поле «**Администрирование Ключей ЭЦП**» В открывшемся меню выбираете свой токен и необходимый ключ на нем.



И вы сможете:

- печать Сертификата открытого ключа ЭЦП клиента;
- смена пароля для доступа к секретному ключу ЭЦП в Хранилище ключей;
- смена наименования секретного ключа ЭЦП в Хранилище ключей;
- удаление секретного ключа ЭЦП из Хранилища ключей.

Вход в систему с использованием USD-токена

Для загрузки Java-апплета «Internet-Банкинг для корпоративных клиентов» подключитесь к Интернет, запустите Web-браузер и перейдите на главную страницу https://ibank.ccb.ru/.

Подключите USB-токен к USB-порту компьютера. Если все сделано правильно (драйвер установлен) USB-токен будет постоянно гореть синим светом.

На главной странице «iBank 2» выберите пункт **«Начать работу / Зарегистрироваться»,** в результате чего сначала загрузится стартовая html-страница, а через 15 - 30 секунд (в зависимости от скорости доступа в Интернет) загрузится АРМ «Internet-Банкинг для корпоративных клиентов», первое окно которого, **Вход в систему,** предназначенное для аутентификации клиента, представлено на рис. 8.

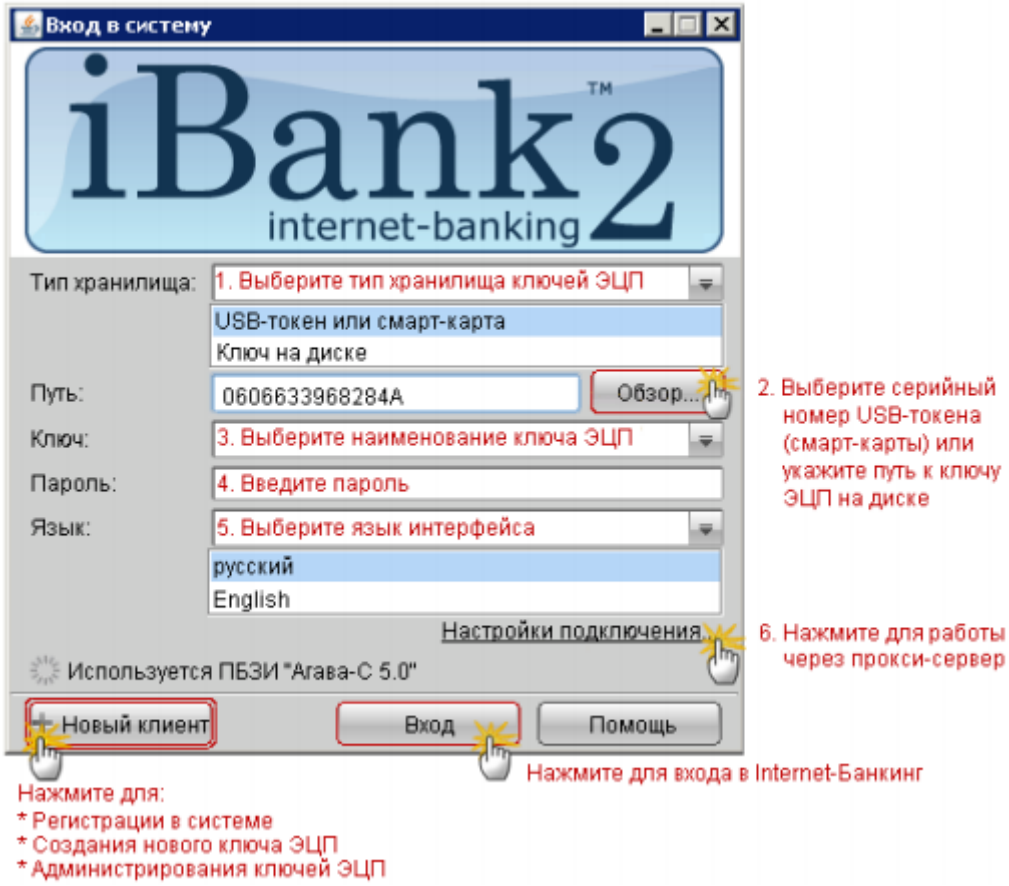


Рис. 8. Окно **Вход в систему.** Аутентификация клиента

- В поле **Тип хранилища:** выберите **USB-токен.** В поле **Путь:** отобразится серийный номер USB-токена. Для выбора другого USB-токена воспользуйтесь кнопкой **Обзор.**
- Из списка поля **Ключ:** выберите наименование секретного ключа ЭЦП. Укажите пароль для доступа к выбранному ключу. При вводе пароля учитываются язык (русский/латиница) и регистр (заглавные/прописные буквы).
- Из списка поля **Профиль** выберите необходимый профиль работы. При выборе профиля **Текущий** загружаются настройки пользователя, сделанные в предыдущем сеансе работы. При выборе профиля **По умолчанию** загружаются настройки апплета, принятые системой по умолчанию.
- Если для подключения к Интернет используется Proxy-сервер введите в поля **адрес** и **порт,** соответственно, адрес и порт Proxy-сервера. Если для подключения Proxy-сервер не используется, снимите метку в поле **Использовать прокси.**
- Для входа в интернет-банк для корпоративных клиентов нажмите кнопку **Вход.**